# Trojan horse resurrected - On the legality of the use of government spyware

Cupa, Basil

# LIVING IN SURVEILLANCE SOCIETIES: **'THE STATE OF SURVEILLANCE'**

Proceedings of LiSS Conference 3

**Edited by:**
C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux

# Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)

*Basil Cupa*[41]

## 1. Introduction

*R2D2* – does this name ring a bell? You are right, it is the famous and much-beloved Star Wars robot. Since October 2011, it also stands for a detected spyware programme used by the German government to infiltrate the computers of suspects. This particular programme is capable of spying on email accounts, of listening in on Internet telephone calls, and even of logging keystrokes or activating webcams. After a few days of public indignation, it became clear that not only the German intelligence and security services made use of such practice, but so did their counterparts in Austria, Switzerland, and The Netherlands. The crucial question regarding this matter, which challenges the rule of law, is whether the use of government spyware was legal. Under German Law, since 2008, there is a fundamental right to digital privacy that entails the confidentiality and integrity of IT systems and therefore, in principle, protects the individual from sting operations. The rightful use of Trojan horse programmes requires *inter alia* the existence of both a substantial public interest as well as a clear and precise legal basis allowing investigation. Regrettably, neither of the two requirements is indisputably fulfilled. Some scholars argue that solely the fight against terrorism constitutes a sufficient public interest, while others claim the combat of extremism or organised crime to be a substantial interest as well. Furthermore, most European states will have in common the fact that possible legal bases do not (yet) address the use of Trojan horse programmes specifically. General rules, such as those on telephone tapping, turn out to be too abstract and hence they are too weak to justify interference with fundamental rights. In consequence, the individual is – without his knowledge – confronted with illegal government action, which calls for public scrutiny and a broader political will to create sufficient legal bases.

## 2. Technical Aspects

Besides its military origin in ancient times, the term ‘Trojan horse’ came to be used again in high frequency around a year ago in the context of information technology (IT). The modern term ‘Trojan horse’ denotes a computer programme used by government officials for the purpose of covert investigation of serious crimes, without the suspect’s knowledge or consent, thereby

[41]*Basil Cupa, University of Zurich, Switzerland*

enabling access to third-party IT systems. From a technical point of view, the Trojan is camouflaged as a harmless programme or useful file, but is in fact a virus dropper, which carries an independently working spyware source code that mostly executes undesirable, additional functions unknown to the user (Bucher, 2010: 16 et seq.). Once the spy is successfully placed, it can telecontrol the infiltrated system and execute all kinds of actions, which normally only the user is able to trigger, via a so-called 'backdoor' access. This basically means that the controller can remotely explore all data residing on the suspect's computer, modify or delete data, and even upload new files (Kaspersky, 2008: 63). Another common spyware feature is a *keylogger* that monitors keystrokes, especially usernames and passwords (Holzner, 2009: 14). According to government officials, the main goal, however, is not comprehensive online search but 'just' so-called 'source telecommunication surveillance'. This investigation method is considered necessary due to Voice-over-Internet-Protocol services (VoIP), such as MSN or Skype, popular amongst presumed terrorists and other felons. While making an online call or sending a file over VoIP, the data to be transferred is nearly irreversibly encrypted, even to profound IT specialists. With the help of a Trojan, it is yet much easier to collect the desired data directly on the suspect's computer before encipherment, prima facie avoiding unnecessary resources for a hardly promising endeavour to intercept the data transfer via VoIP services (Porter / Gough 2007: 309).

The Trojan *R2D2* probably used by the German Federal Criminal Police Office, as well as the Bavarian Criminal Police Bureau, and Swiss authorities (Chaos Computer Club 2011: 4; Fox 2012: 1; Federal Council of Switzerland 2011: 1) comprises a software library that primarily acts as a Skype enhancement, enabling the interception of Internet phone calls. Beyond that, all common features for a comprehensive online search are in place. Even if some functions have been deactivated, for example the keylogger, the controlling server could easily activate them. Furthermore, several code fragments of *R2D2* have been detected whose abilities are still unknown (Dewald et al. 2011: 4, 6). In five Bavarian cases, for instance, it is ascertained that the Criminal Police Bureau made indeed use of far-reaching spyware options when taking screenshots from Firewall Internet browsers, reaching up to 66,000 shots in one case (Fox, 2012: 1; Fröhner, 2012: 118). Given the potential severity of Trojan-based surveillance measures, the crucial question is whether the use of such practices is legal or not.

## 3. Legality

To outline the legal framework of all respective Central European countries in which *R2D2* has been used, or is presumed to be used, would reach too far in the context of the present contribution. However, if we approach the question of legality of government spyware (officially called 'Remote Forensic Software') from a more basic perspective, then a set of common criteria justifying the limitation of fundamental rights can be identified (Kaolin/Künzli, 2008: 115; Villiger, 1999: 344), e.g. in Article 8 (2) ECHR, Article 36 of the Federal Constitution of the Swiss Confederation (hereafter: CF) or Article 19 of the Basic Law for the Federal Republic of Germany (hereafter: GG). The aim of this paper is to give a brief survey of this set of common legality requirements for the use of Trojan horse programmes.

## 3.1 Extended Fundamental Rights Protection

As far as is known, the ECtHR has not yet ruled on the legality of Trojan horses or online searches specifically. However, such a case could reach the court in the future and would have to be examined under Article 8 ECHR, which guarantees *inter alia* a right of everyone to privacy (ECtHR, *Klass vs. Germany*, nr. 5029/71 of 09.06.1978, § 41; see further Kälin/Künzli, 2008: 435 et seq.; Tschentscher, 2008: 387). The scope of protection is granted to those whose data is collected, saved, passed on or processed, if it concerns private life outside the public sphere (Grabenwarter/Pabel, 2012: 231). Following the jurisprudence of the Federal Constitutional Court of Germany to Article 1 (1) in conjunction with Article 2 (1) and Article 10 GG (BVerfG, 1 BvR 370/07 of 27.02.2008, headnote 4), the broad scope of Article 8 ECHR, which aims at free and unhindered personality development, could as well be interpreted to encompass a fundamental right to the guarantee of the confidentiality and integrity of IT systems. By now, computers are not any longer used for work purposes only, but also serve for private communication and thereby contribute to elementary personal development in multiple ways. For this simple reason, a broader perspective on fundamental rights protection is deemed inevitable. Not all European countries did yet take this step. In Switzerland, for example, the Federal Supreme Court did so far not have the chance to rule upon whether citizens are protected against the use of Trojans by a specific form of the right to privacy and telecommunications secrecy or even a new and unwritten fundamental right such as the right to the guarantee of the confidentiality and integrity of IT systems. One may justly assume that the Federal Supreme Court would extend the right to privacy, laid down in Article 13 CF, due to the immense potential threat to freedom and democracy inherent in Trojans. The consequence of such qualification would be that the state had to restrain from interference with the citizen's private life on IT systems, especially the intimate sphere as the very essence of privacy (Tschentscher, 2008: 393). As will be shown below, an encroachment on this right could potentially be justified by the legislature, if based on a sufficient legal basis, justified by a public interest, and strictly respects the proportionality of means as well as the minimum core content of fundamental rights.

## 3.2 Weak Legal Bases

Whether or not there is a sufficient legal basis for the use of Trojans is controversially debated and therefore one of the crucial issues when talking about this new method of government surveillance. According to the legality principle, states are required to allow encroachment on fundamental rights only if provided for by law, formulated clearly and precisely in a general-abstract way, in order to ensure the foreseeability and certainty on the law (Villiger, 1999: 346). Particular attention to this principle has to be paid in course of criminal investigation, where Trojans operate (Böckenförde, 2008: 929). Anyone must be able to anticipate with a certain degree of predictability *when* and *in which way* Trojans may be used. The requirements of clarity and foreseeability must be dealt with even more strictly, due to the secret nature of investigation (ECtHR, *Kvasnica vs. Slovakia*, nr. 72094/01 of 09.06.2009, § 79). This means explicitly that national law must specify where government spyware may be installed, for the investigation of which category of crimes this shall be allowed, and for how long surveillance measures may endure. Beyond that, procedural measures must ensure complete documentation of the collected data and its entire disclosure to the defendant and the court after the ending of the operation, so

that the suspect's procedural rights remain respected. Furthermore, the whole process from collection until disclosure of data has to be supervised by an independent authority (ECtHR, *Calmanovici vs. Romania*, nr. 42250/02 of 01.07.2008, § 121). But, does national legislation fulfil these requirements?

In Germany, the whole debate on this topic as well as the legislative process are the most advanced. The Act on the Federal Criminal Police Office (hereafter: BKAG) contains a legal basis that allows covert investigations without the suspect's knowledge for the purpose of a so-called 'online search', whereby the legislature deliberately intended to include the use of technical means such as Trojans into the current version of Paragraph 20k. According to the intention of the legislature, all data not relating to the suspect's intimate sphere may be collected and passed on to the controller's server. Besides, the use of keyloggers shall be allowed, whereas activating microphones and webcams is prohibited (Draft bill BKAG 2008: 29). Paragraph 20k (1) and (4) state that surveillance measures may be directed against persons creating a danger for life and freedom of others or against those who endanger the existence of the state or people. This formulation though appears quite vague because the bill does furthermore not contain a list with at least the categories of crime a person must be suspected of, not to mention a precise enumeration of every respective single crime in the penal code. Thus, it is not clear from the wording whether Trojans are allowed to be used only in the case of terrorism or as well, for example, in the case of less serious drug offences. On the more positive side, the bill prescribes a maximum time limit for investigation of three months and a detailed documentation procedure in Paragraph 20k (6) and (7). Given the potential severity of the encroachment on privacy rights, the required clarity and foreseeability of the legal basis remain questionable (note that the distinction between preventive and repressive investigation is as well of a certain importance, cf. Albrecht/Dienst, 2012: §§ 9 et seq.). Against this background, it is not surprising that a constitutional complaint for partial annulment of the BKAG is currently pending before the Federal Constitutional Court (BVerfG, 1 BvR 966/09 and 1 BvR 1140/09, to be decided in 2012).

Even though the example outlined above is not free from dispute, there are other, even more material violations of law. In the majority of cases, there is no specific legal basis for the use of Trojans and prosecution services therefore try to invoke the established provisions on telephone surveillance (Hansjakob, 2011: 4), as seen in Switzerland with Article 280 of the Swiss Criminal Procedure Code (hereafter: CPC). The next question thus is whether provisions on telephone surveillance could, in principle, constitute a sufficient legal basis for the use of Trojans, or not.

## 3.3 Prohibition of Analogy

If the use of Trojans and established telecommunication surveillance are the same, exactly the same provisions must apply. If they are not the same, but are comparable, and there are no specific provisions on the use of Trojans, this legal loophole is in principle to be closed by analogy (Kramer 2005: 174, 178). But if the use of Trojans and established telecommunication surveillance are neither the same nor comparable, it is inadmissible from the outset to apply the same provisions. First of all, the use of Trojans works differently compared to established telecommunication surveillance where the mobile service provider is obliged to enable access to

transfer data. It is widely recognised that these are two different issues (cf. Fraenkel/Hammer, 2011: 889; Métille, 2011: 3, 7). The crucial question concerns their comparability. Whether or not comparability is possible, has to be decided in an overall consideration based on technical configuration and determined by the goal and severity of the intervention. Just looking at the goal of intervention, both means of surveillance *inter alia* aim at the prevention of terrorism or other serious crimes and therefore appear comparable at first sight. Seen from the technical point of view, and from the potential severity of an intervention, the two investigation methods suddenly appear to be different. Trojans implement spyware that is designed to enable online searches as well as source telecommunication surveillance. While online searches allow the controller to perform all commands normally only the user is able to trigger, source telecommunication surveillance 'only' concerns Internet telephone calls – at least theoretically (Fox, 2012: 1).

In fact, online searches and source telecommunication are not so different. Source telecommunication surveillance takes either place during a VoIP conversation or after the phone call via secret access to the VoIP log saved on the computer. Intruding into a third party's IT system signifies at any rate the realisation of a general communication risk. With this step of infiltration, a point of no return is passed, since not all data of a suspected criminal is designed for communication. What if a message is written on Skype's chat box, but not sent? The message has the quality of an unspoken thought and thoughts must never be controlled. As we saw, not all data on a computer is necessarily communicated. The process of infiltration is, taken for itself, therefore already a more far-reaching intervention than the surveillance of established means of telecommunication (Abate, 2011: 125). Besides, technical possibilities to restrict basic spyware functions to a secured minimum are still in question. As seen with the example of *R2D2*, its source code contained more functions than required for the intended source telecommunication surveillance (Dewald et al. 2011: 3 et seq.). The fact that some of these functions were deactivated is irrelevant, because they can easily be activated at any time without major effort on the controller's end. The deactivated parts of the spyware source code constitute huge potential for abuse that cannot be forestalled by simple deactivation. This aspect increases the severity of an intervention and is another reason why Trojans are not directly comparable, e.g., to the surveillance of a fixed-line phone call.

However, not all lawyers share this point of view. The Regional Court of Hamburg, e.g., assumed comparability between established and source telecommunication surveillance (LG Hamburg, 608 Qs 17/10 of 13.09.2010, § 2 c/bb). And so did the Regional Court of Landshut, but with the specification that taking screenshots goes beyond what is comparable to established telecommunication surveillance (LG Landshut, 4 Qs 346/10 of 20.01.2011, § 1). Even though not everyone may agree with the court's fundamental theoretical postulate, the judgment correctly confirms that screenshots are a far-reaching intervention, which goes beyond established means of surveillance (Ibid. § 3). If this conclusion is correct for taking screenshots, this must *a minori ad maius* apply to online searches as a whole. Neither source telecommunication surveillance nor online searches are comparable to surveillance by interception, because they both require the infiltration of an IT system, which in itself already constitutes a new, so far unseen quality of intervention (cf. as well for this point of view Abate, 2011: 125; Hansjakob, 2011: 4). And all those who still think one could apply the provisions on established means of telecommunication surveillance should ask themselves the following

question: What is the purpose of extended fundamental rights protection, if the former provisions on telecommunication surveillance shall now apply by analogy?

## 3.4 Variety of Legitimate Aims

According to Swiss doctrine to Article 36 (2) CF, any public interest is in principle sufficient to justify encroachment on fundamental rights (Métille, 2011: 4). The German doctrine is slightly more restrictive and, *inter alia*, requires the public interest to find expression within the constitution (Rohloff, 2008: 221). At European level, a restriction on the fundamental right to privacy and the guarantee of the confidentiality and integrity of information technological systems is *a priori* considered to be of a certain severity, so that no public interest debate is suitable to justify restriction. In Article 8 (2) ECHR, this point of view is laid down in law. It states in a much-noted formula that only interests of national security, public safety or the economic well-being of the state, as well as the prevention of crime, the protection of health or morals, and the protection of the rights and freedoms of others may justify encroachment. With the use of Trojans, a twofold aim is pursued, namely the safeguard of national and public security, as well as the prevention of crime. Interestingly, German law has special rules for the restriction of the right to privacy in Article 10 (2) in conjunction with Article 19 (4) GG, which are similar to Article 8 (2) ECHR, but are formulated more strictly. Only the safeguard of democracy, public safety or the existence of the state is considered substantial enough to constitute a legitimate aim. Trojans can be used to pursue these legitimate security aims, but for which categories of crime their use is legitimate, for instance terrorism or child pornography, is a question of proportionality (BVerfG, 1 BvR 370/07 of 27.02.2008, §§ 219 et seq.).

## 3.5 Disproportionate Trade-off

Interference by a public authority with fundamental rights is justified, if the way of reaching a legitimate aim is useful, necessary, and reasonable – or in other words: proportionate (Grabenwarter/Pabel, 2012: 252; Métille, 2011: 4). The use of Trojans is certainly useful and expedient to generate data on potential criminals and for this reason contributes to crime prevention. But is their use necessary and reasonable, if we balance the interest of citizens and privacy against the interest of public safety? Previously in 1978, the ECtHR saw the need for surveillance measures due to new forms of terrorism. What the court said thirty-four years ago appears to be even truer today – at least intuitively. At the same time, the judges emphasised that security is not a self-sufficient goal. The huge potential danger of abuse inherent to surveillance requires the national legislature to put several safety precautions in place (ECtHR, *Klass vs. Germany*, nr. 5029/71 of 09.06.1978, § 49). As a first measure of precaution, surveillance shall not be allowed in a general and preventive way (Métille, 2011: 3). Additionally, it also appears convincing that there must be a reasonable suspicion of illegal behaviour in combination with a real and urgent threat to higher-ranking legal interest, such as, for example, the prevention of a terror attack (BVerfG, 1 BvR 370/07 of 27.02.2008, § 266). But one question still remains: Which categories of crime warrant the use of Trojans? The answer to this question is in any case political. The most important point is that the legislature gives us clear and precise guidelines (as well Fox, 2012: 1). Even though contrary to the ruling of the Federal Constitutional Court of

Germany, which expressed the view that the requirement of a real and urgent threat to higher-ranking legal interests is a high enough hurdle to forestall abusive effects (BVerfG, 1 BvR 370/07 of 27.02.2008, §§ 219, 327), there are good reasons to allow the use of Trojans only in case of serious crimes against the state. If one compares the individual's interest not to be monitored with the public interest of crime prevention, this trade-off may be comprehensible. However, if one compares the public's interest of not being monitored, with the public interest of crime prevention, it is less obvious which interest is higher-ranking. Then society as a whole should not live under the fear of surveillance – and neither should petty criminals. If people know that Trojans are used only for the prevention of the most serious crimes, they will not feel threatened by surveillance. If Trojans are as well used for the investigation of smaller crimes, the public may begin to behave differently because they feel an inconceivable danger of potential surveillance (cf. Kutscha, 2007: 1171). Drug crimes, for instance, appear gross at first glance. But, compared to terrorism they appear petty. Therefore, to investigate smaller crimes with the help of Trojans is neither necessary nor reasonable. Their use is only proportionate for the investigation of the objectively most serious crimes. Nevertheless, this balancing of legally protected interests is in the end a political question and should therefore be decided as precisely as possible by the legislature.

Another less disputed measure of precaution is to allow Trojans upon granting of a judicial order. Due to the fact that Trojans are used secretly, an independent review should take place in advance, to examine the compliance with the requirements laid down by the law. This ensures a certain safeguard for the procedural rights of the affected person, because the suspect himself is not able to question the legality of surveillance at the moment the intervention takes place (Fraenkel/Hammer 2011: 889). After the intervention took place, the persons affected by surveillance should be informed about the measure, if there is not a serious public interest to restrain from doing so. Besides, procedural rights must be respected and enforced by a sufficient retrospective legal monitoring mechanism (ECtHR, *Klass vs. Germany*, nr. 5029/71 of 09.06.1978, §§ 59 et seq.). Finally, general data protection must be ensured as far as possible and the acquisition of new investigation technology – as is the case for Trojan horse programmes – must be presented to the responsible authority for data protection (Fraenkel/ Hammer 2011: 888). Due to the *ultima ratio* character and the principle of subsidiarity applying to surveillance measures, there is a simple and less far-reaching alternative, if the requirements for the use of Trojans are not clearly fulfilled: one may seize a suspect's computer (ECtHR, *Stefanov vs.* Bulgaria, nr. 65755/01 of 22.08.2008, §§ 16 et seq.).

## 3.6 Core Content of Privacy

Is it permissible to collect all kinds of data from the computer of a suspect? If this is not the case, which data may be monitored and collected? Independent of whether data is communicated, designed to be communicated in the future or simply residing on a computer without any intent to be transferred, intimate data must under no circumstances be monitored (Desoi/Knierim, 2011: 399). This also applies to all information about the sexual sphere or the most inner feelings of a person, as well as diaries or pure interpersonal communication without any connection to the suspected crime (Frowein/Peukert, 2009: 289). This means specifically that there are no higher-ranking interests *per se*, which could justify interfering with the intimate sphere of a person, even

if this person is a highly dangerous criminal. The protection of this sphere is considered absolute and must always be respected (cf. Article 19 (2) GG as well as Article 36 (4) CF). The Federal Constitutional Court of Germany pointed out that the best technical means not to collect intimate data should be employed. If, however, such highly sensitive information is unwittingly collected in the context of the infiltration of an IT system, it must be deleted immediately (BVerfG, 1 BvR 370/07 of 27.02.2008, §§ 280 et seq.). In a Bavarian case where several thousand screenshots were taken automatically every thirty seconds, the court found a serious threat to the core content of privacy (LG Landshut, 4 Qs 346/10 of 20.01.2011, §§ 3a, 4).

## 4. Conclusion

In 2008, the Federal Constitutional Court of Germany created a new a fundamental right to guarantee the confidentiality and integrity of information technological systems (BVerfG, 1 BvR 370/07 of 27.02.2008). This judgment is of great importance as the court's extended fundamental rights approach protects everyone against the use of Trojans. Besides, the judgment may serve as a precedent for similar tendencies in other countries. *De lege lata*, there are – except for the German BKAG – no rules addressing the use of Trojan horse programmes specifically. However, there are other provisions, which are argued to serve as a sufficient legal basis for the use of Trojans. In the majority of cases, a significant number of lawyers and authorities are of the opinion that the rules on established telecommunication surveillance apply to the use of Trojans by analogy. This point of view needs to be refused, based on the fact that the infiltration of a suspect's computer has a new, so far unseen quality, to which a huge potential of abuse is inherent that goes beyond the severity of established means of surveillance. The use of Trojans is not comparable to the surveillance of, for instance, a fixed-line telephone and hence an analogous application of the existing legal bases is incorrect. If one nevertheless applies them by analogy, there is a lack of clarity and precision in the wording, which stands in contradiction to the principle of legality. The next challenge is to comply with the proportionality principle. Trojans must only be used in cases of a real and urgent threat to higher-ranking legal interest, such as the prevention of terrorism or the safeguard of democracy. Though, it has to be mentioned that it is a political trade-off for which categories of crime the use of Trojans shall be legitimatised. Less disputed is the need to protect the intimate sphere as the core of privacy, at any time, under any circumstances. In summary, the question of legality depends upon a plethora of factors and remains so for the time being. Based on our previous analysis, we can distil the following three core theses:

1. Fundamental rights can and must be interpreted in a way that grants protection against the use of Trojan horse programmes.
2. A sufficient legal basis for the use of Trojan horse programmes cannot be 'created' by analogy.
3. Due to the severity of intervention, Trojan horse programmes should only be used to prevent terrorism or to safeguard the existence of democracy.

The practical consequence of this analysis is: If evidence is obtained by illegal means, it may, according to the theory of the poisonous tree, not be used against the accused (Meyer-Goßner/Cierniak, 2010: 375).

## References


Abate, C., (2011), *Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail*, Datenschutz und Datensicherheit (DuD), 2/2011, 122.

Albrecht, F., Dienst, S., (2012), *Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme*, JurPC, Web-Dok. 5/2012, §§ 1-65.

Böckenförde, T., (2008), *Auf dem Weg zur elektronischen Privatsphäre*, Juristenzeitung (JZ), 19/2008, 925.

Bucher, M., (2010) *Spyware: Rechtliche Würdigung ausgewählter Fragen sowie Empfehlungen an die Praxis unter besonderer Berücksichtigung des Eidgenössischen Datenschutzgesetzes*, Zurich / Basel / Geneva: Schulthess.

Chaos Computer Club, *Ozapftis – Teil 2: Analyse einer Regierungs-Malware vom 26. Oktober 2011*, available at: www.ccc.de.

Desoi, M., Knierim, A., (2011), *Intimsphäre und Kernbereichsschutz*, Die Öffentliche Verwaltung (DÖV), 10/2011, 398.

Dewald, A., Freiling, F. C., Schreck, T., Spreitzenbarth, M., Stüttgen, J., Vömel, S., Willems, C., (2011), *Analyse und Vergleich von BckR2D2-I und II,* University of Erlangen, Dept. of Computer Science, Technical Reports, CS-2011-08.

Draft Bill BKAG: Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/10121 vom 13.08.2008.

Federal Commissioner for Data Protection, *Inoffizieller Bericht gemäß § 26 Abs. 2 Datenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes vom 31. Januar 2012*.

Federal Council of Switzerland, Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen, Medienmitteilung vom 23. November 2011.

Fox, D.,*Untragbar unerträglich*, Datenschutz und Datensicherheit (DuD), 1/2012.

Fraenkel, R., Hammer, V., (2011), *Vom Staats- zum Verfassungstrojaner*, Datenschutz und Datensicherheit (DuD), 12/2011, 887.

Fröhner, H., (2012), *Kapitalismus*, Berlin: epubli.

Frowein, J. A., Peukert, W., (2009), *Europäische MenschenRechtsKonvention*, 3rd ed., Kehl: Engel.

Grabenwarter, C., Pabel, K., (2012), *Europäische Menschenrechtskonvention*, 5th ed., Munich / Basel / Vienna: C.H. Beck / Helbing Lichtenhahn/Manz'sche.

Hansjakob, T., (2011), *Einsatz von GovWare – zulässig oder nicht?*, Jusletter vom 05. December, 2011.

Holzer, S., (2009), *Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts*, Kenzingen: Centaurus.

Kälin, W. Künzli, J. (2008), Universeller Menschenrechtsschutz, 2nd ed., Basel: Helbing Lichtenhahn/Nomos.

Kaspersky, E., (2008), *Malware*, Munich: Carl Hansen Publishing.

Kramer, E. A., (2005), *Juristische Methodenlehre*, 2nd ed.

Kutscha, M., Verdeckte., "Online-Durchsuchung" und Unverletzlichkeit der Wohnung, Neue Juristische Wochenschrift (NJW), 17/2007, 1169.

Meyer-Goßner, L, Cierniak, J., (2010), *Strafprozessordnung*, Munich: H.C. Beck.

Métille, S., (2011), *Les mesures de surveillance prévues par le CPP*, Jusletter vom 19.

December 2011.
Porter, T., Gough, M., (2007), *How to cheat at VoIP Security*, Rockland (MA): Syngress Publishing.
Rohloff, A., Grundrechtsschranken in Deutschland und den USA, Doctoral Thesis at the University of Konstanz 2006, Munster: LIT, 2008.
Tschentscher, A., *Das Grundrecht auf Computerschutz*, Aktuelle Juristische Praxis (AJP), 4/2008, 383.
Villiger, M. E., (1999), *Handbuch der Europäischen Menschenrechtskonvention (EMRK)*, 2nd ed., Zurich: Schulthess.